Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé

Délibération n° 51/2019 du 18.10.2019

Conformément à l'article 57 paragraphe (1) lettre (c) du règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après désigné « le RGPD »), chaque autorité de contrôle a pour mission de conseiller « *conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement* ». L'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données prévoit précisément que la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») exerce les missions dont elle est investie en vertu de l'article 57 du RGPD.

Par courrier en date du 26 juillet 2019, Monsieur le Ministre de la Sécurité Sociale a fait parvenir à la Commission nationale une série de propositions d'amendements au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé (ci-après « les amendements »), ainsi qu'un texte coordonné dudit projet de règlement grand-ducal.

Pour rappel, la CNPD a rendu, le 5 avril 2018[1], un premier avis relatif au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé (ci-après « le projet de règlement grand-ducal ») dans lequel elle a formulé toute une série d'observations sur les dispositions dudit projet ayant une répercussion sur le respect de la vie privée et la protection des données à caractère personnel.

Le Conseil d'Etat quant à lui s'est prononcé sur le projet de règlement grand-ducal dans un avis rendu le 23 octobre 2018, dans lequel il a repris de nombreuses critiques émises par la Commission nationale dans son avis précité du 5 avril 2018.

La Commission nationale se félicite du fait que certaines de ses remarques ont été prises en compte par les auteurs des amendements.

I. Remarques préliminaires

a. Principe de licéité d'un traitement de données à caractère personnel

Dans son avis du 5 avril 2018, la CNPD a considéré qu'au vu du principe de licéité d'un traitement de données à caractère personnel qui doit être lu à la lumière de l'article 8 paragraphe (2) de la Convention européenne des droits de l'homme concernant le droit au respect de la vie privée, ainsi que de l'article 52 paragraphes (1) et (2) de la Charte des droits

[1] Délibération n° 242/2018 du 5 avril 2018.

fondamentaux de l'Union européenne[2], au moins les dispositions concernant la durée de conservation des données au dossier de soins partagé (ci-après : « DSP »), les droits des titulaires mineurs non émancipés et titulaires majeurs protégés par la loi, ainsi que la limitation du droit d'accès et du droit à l'effacement devraient être prévues dans la loi au sens stricte du terme et plus précisément par l'article 60*quater* du Code de la sécurité sociale, et non pas dans un acte réglementaire.

Tout d'abord, la CNPD remarque que les dispositions sur la durée de conservation des données à caractère personnel au DSP sont toujours prévues aux articles 4 et 9 paragraphe (5) du projet de règlement grand-ducal amendé.

Par ailleurs, par l'amendement 7, les auteurs ont supprimé l'article 7 du projet de règlement grand-ducal concernant les titulaires mineurs non émancipés et titulaires majeurs protégés par la loi pour les raisons suivantes : *« Les avis du Conseil d'Etat et de la Commission nationale pour la protection des données établissent que l'article 7, du moins en partie, déroge aux règles relatives aux mineurs et aux majeurs protégés par la loi telles que prévues au Code civil.*

Ainsi dans un souci du respect de la hiérarchie des normes, l'article 7 est supprimé, les dispositions qui introduisent des droits spécifiques pour certains mineurs devant être reprises dans les lois particulières régissant leurs droits. »

En ce qui concerne une limitation des droits des personnes concernées, comme notamment le droit d'accès, l'article 23 paragraphe (1) du RGPD dispose que le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter, entre autres, la portée du droit d'accès prévu par l'article 15 du RGPD. Une telle limitation doit respecter l'essence des libertés et droits fondamentaux et elle doit constituer une mesure nécessaire et proportionnée dans une société démocratique pour garantir un des dix motifs y prévus. Une mesure législative limitative doit d'ailleurs contenir certaines dispositions spécifiques énumérées à l'article 23 paragraphe (2) du RGDP.

Dans son avis du 5 avril 2018, la CNPD avait remarqué que comme l'article 9 paragraphe (2) du projet en sa version initiale limitait le droit d'accès des titulaires, représentants légaux et médecins référents, cette limitation devrait être prévue par une loi au sens stricte du terme et respecter les exigences susmentionnées prévues à l'article 23 du RGPD. Par son amendement 8, les auteurs expliquent que comme le nouvel article 7 paragraphe (4) « *prévoit de rendre inaccessibles au titulaire certaines données pouvant causer le cas échéant un préjudice grave pour sa santé, [il] est supprimé suite à l'avis précité du Conseil d'Etat vu qu'il restreint les droits d'accès du titulaire à son dossier de soins partagés, tels qu'attribués par la base légale qu'est l'article 60quater du Code de la sécurité sociale.* »

Hormis les articles concernant la durée de conservation des données, la CNPD constate donc que ses autres recommandations concernant les dispositions pour lesquelles un cadre réglementaire n'est pas suffisant, mais où un encadrement par une loi au sens stricte du terme est requis, ont été prises en compte par les auteurs des amendements du projet de règlement grand-ducal. Or, elle regrette qu'après plus de 17 mois après l'adoption de son avis précité, aucun projet de loi n'ait été déposé à la Chambre des Députés, en vue d'adopter les mesures législatives nécessaires pour prendre en compte lesdites considérations La CNPD profite par ailleurs de l'occasion pour réitérer sa recommandation émise au législateur dans le cadre de

[2] Pour plus de détails, la CNPD renvoie à son avis du 5 avril 2018.

son avis du 5 avril 2018 de s'inspirer du Code de la santé publique français afin de prévoir dans la législation luxembourgeoise des sanctions pénales en cas d'abus d'accès au DSP.

b. La question de la responsabilité du traitement

L'article 60*ter* paragraphe (4) du Code de la sécurité sociale prévoit que l'Agence nationale des informations partagées dans le domaine de la santé (ci-après désignée « l'Agence eSanté ») a la qualité de responsable du traitement des données à caractère personnel au sens de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, loi abrogée par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Or, la CNPD a déjà estimé à maintes reprises[3] que la responsabilité unique de l'Agence eSanté concernant les traitements des données à caractère personnel contenues dans le DSP ne correspond pas à la réalité tel que le système est envisagé. En effet, il ressort de l'économie générale de la loi du 17 décembre 2010 portant réforme du système de soins de santé que l'Agence eSanté d'un côté, et les professionnels de santé d'autre côté, participent conjointement à la réalisation des finalités et des moyens du traitement tels que définis par le législateur. L'article 26 paragraphe (1) du RGPD exige que « *les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis.* »

La Cour de Justice de l'Union européenne a pris position à l'égard de la notion de « responsabilité conjointe » dans un arrêt récent en jugeant que son existence « *ne se traduit pas nécessairement par une responsabilité équivalente, pour un même traitement de données à caractère personnel, des différents acteurs. Au contraire, ces acteurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce.* »[4]

La CNPD constate dans ce contexte que les auteurs des amendements ont pris conscience que ce n'est pas uniquement l'Agence eSanté qui est à considérer comme responsable du traitement, mais que différents acteurs assument différentes responsabilités en ce qui concerne le traitement des données contenues dans le DSP. En effet, le commentaire de l'amendement 8 mentionne les obligations et responsabilités des professionnels de santé intervenant dans la prise en charge médicale du patient leur incombant en vertu de l'article 13 du RGPD, tandis que l'amendement 2 prévoit les obligations et responsabilités de l'Agence eSanté en vertu de l'article 14 du RGPD. Les auteurs expliquent dans ledit commentaire que ces précisions poursuivent « *la même volonté de déterminer clairement les obligations et responsabilités des différents intervenants en vertu de l'article 26 du règlement (UE) 2016/679 comme préconisé par le Conseil d'Etat et la Commission nationale pour la protection des données dans leurs avis respectifs.* »

---

3 Voir la délibération n° 345/2010 du 24 novembre 2010 relatif au projet de loi n°6196 portant réforme du système de soins de santé, ainsi que la délibération n° 242/2018 du 5 avril 2018 sur le projet de règlement grand-ducal sous examen.

4 Arrêt du 29 juillet 2019, Fashion ID GmbG & Co. KG / Verbraucherzentrale NRW eV, C-40/17, EU:C:2018:1039, point 70; voir, en ce sens, arrêt du 10 juillet 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, point 66.

Par ailleurs, les paragraphes (3) alinéa 4 et (5) de l'article 6 du texte coordonné du projet de règlement grand-ducal prévoient que le droit à l'effacement, respectivement le droit d'obtenir la rectification des données inexactes ou incomplètes dans son DSP, doivent être exercés soit auprès du professionnel de santé, soit auprès de l'Agence eSanté.

Finalement, dans sa version actuelle, l'article 10 paragraphe (2) du projet de règlement grand-ducal concernant la sécurité de la plateforme mentionne que le prestataire est à considérer comme responsable du traitement et qu'il peut recourir à des sous-traitants afin de mettre en œuvre les mesures techniques et organisationnelles de sécurité appropriées afin de garantir un niveau de sécurité adapté aux risques. Des précisions quant à la notion d'un « prestataire » se retrouvaient dans le commentaire des articles de la version initiale du projet de règlement grand-ducal : « *Vu la diversité des prestataires susceptibles de se connecter à la plateforme ou d'utiliser l'une de ses applications, à savoir un établissement hospitalier, une pharmacie, un laboratoire d'analyses médicales et de biologie clinique, une association de médecins ou un cabinet individuel et, pour les données mentionnées à l'article 60quater, paragraphe 2 du Code de la sécurité sociale, un réseau d'aides et de soins, un centre semi-stationnaire, un établissement d'aides et de soins, un établissement à séjour intermittent [...]* ». Or, la CNPD avait recommandé aux auteurs d'ajouter une définition dudit terme à l'article 1er du projet.

Ainsi, non seulement l'Agence eSanté et les professionnels de santé peuvent, en fonction du traitement en cause, être considérés comme responsables du traitement des données contenues dans le DSP, mais aussi d'autres entités comme celles mentionnées ci-dessus.

La CNPD ne peut que soutenir l'approche des auteurs des amendements de préciser dans le corps du texte les obligations respectives des différentes responsables du traitement comme exigé par l'article 26 du RGPD. Néanmoins, comme on est clairement en présence d'une responsabilité conjointe et non pas d'une responsabilité unique de l'Agence eSanté, la CNPD estime nécessaire de modifier l'article 60*ter* (4) du Code de la sécurité sociale afin de prévoir les responsabilités des différents intervenants.

II. Ad Amendement 2

L'article 2 paragraphe (2) du projet de règlement grand-ducal mentionne toujours que le patient non affilié bénéficiant de soins de santé par un prestataire de soins établi au Luxembourg peut demander l'ouverture d'un DSP moyennant un formulaire de demande à adresser à l'Agence eSanté. Le commentaire des articles de la version initiale du projet de règlement grand-ducal précisait à cet égard que ledit formulaire doit être accompagné des « *pièces justificatives nécessaires* ». Or, au vu du principe de proportionnalité et de nécessité (principe de minimisation des données prévu à l'article 5 paragraphe (1) lettre c) du RGPD), la CNPD a considéré dans son avis du 5 avril 2018 que cette définition manque de clarté et de précision et elle a estimé nécessaire d'énumérer de manière plus précise et concise ces *« pièces justificatives nécessaires »* dans le corps du texte. Or, les auteurs des amendements n'ont pas tenu compte de cette remarque de la Commission nationale.

Par ailleurs, même si l'article 2, paragraphe (3), lettre f) nouveau précise dorénavant que le patient est également informé par l'Agence eSanté du contenu de son DSP au moment de son activation, la Commission nationale se demande toujours quel est ce contenu, c'est-à-dire quelles sont les catégories de données qui sont contenues dans le DSP lors de son activation. Comme dans son avis du 5 avril 2018, elle se pose toujours la question si les données issues

des annuaires référentiels d'identification des patients et des prestataires de soins seront aussi intégrées dans les DSP et dans l'affirmative, elle estime que ces catégories de données devraient être ajoutées à celles déjà prévues à l'annexe 1 du projet de règlement grand-ducal sous le numéro (2).

III. Ad Amendement 4

L'amendement 4 vise à modifier l'article 4 du projet de règlement grand-ducal concernant la fermeture et la suppression du DSP. De manière générale, la CNPD renvoie à ses commentaires formulés dans son avis du 5 avril 2019 concernant la durée de conservation des données suite à la fermeture du DSP, dans lequel elle a considéré qu'une durée d'archivage intermédiaire des données de dix ans apparaît comme excédant celle nécessaire au regard des finalités d'exercice du droit d'accès et d'une éventuelle réouverture du DSP et qu'une durée de conservation des données de cinq ans suite à une fermeture d'un DSP serait plus appropriée et respecterait le principe de la limitation de conservation prévu par l'article 5 paragraphe (1) lettre e) du RGPD.

Par ailleurs, le paragraphe (3) de l'article 4 du projet énonce toujours que seuls les données du DSP « *sont supprimées* » dix ans après la fermeture du DSP à défaut de réouverture endéans ce délai. La CNPD tient à réitérer que non seulement les données doivent être supprimées du DSP, mais que le DSP en lui-même doit être détruit intégralement, comme le prévoit d'ailleurs l'article R1111-34 du Code de la santé publique français.

De même, la CNPD estime qu'il est primordial qu'en cas de clôture d'un DSP, son titulaire soit informé que les données qu'il contient ne seront plus accessibles, d'autant plus que le DSP peut contenir ses volontés en matière de don d'organes, des directives anticipées ou une information relative à des dispositions de fin de vie selon l'article 6 paragraphe (2) lettre b) du projet de règlement grand-ducal.

Finalement, la CNPD tient à répéter qu'il est nécessaire de clarifier dans le projet quelles sont les modalités d'exercice des droits d'accès spécifiques au DSP d'une personne décédée et si, le cas échéant, ces accès s'exerceront conformément à l'article 19 de la loi modifiée du 24 juillet 2014 relative aux droits et obligations du patient.

IV. Ad amendement 5

Le commentaire de l'amendement 5, visant à modifier l'article 5 du projet de règlement grand-ducal concernant l'accès au DSP par les professionnels de santé, précise qu' « *il y a lieu de bien marquer les deux étapes : activation de son compte par le titulaire du dossier de soins partagé et activation de son compte par le professionnel de santé.* » Or, malgré les modifications proposées par l'amendement, il ne ressort toujours pas du projet de règlement grand-ducal si l'activation de son compte sur la plateforme moyennant ses identifiants personnels et la connexion ultérieure est facultative pour les professionnels de santé. Pour cette hypothèse, la CNPD avait déjà constaté dans son avis du 5 avril 2018 qu'il y aurait donc un système « d'opt-out » pour les patients, tandis que pour les professionnels de santé un système « d'opt-in » s'appliquerait.

Finalement, des explications claires des auteurs des amendements sur les acteurs visés par la notion de « collectivité de santé » font encore défaut dans le corps du texte. Dans son avis

du 23 octobre 2018, le Conseil d'Etat a également demandé aux auteurs de préciser les entités visées par la notion de « collectivité de santé ».

V. Ad Amendement 6

Par l'amendement 6, modifiant l'article 6 du projet de règlement grand-ducal encadrant les droits d'accès et d'écriture du titulaire, les auteurs ont pris en compte l'importance de l'autodétermination informationnelle du patient en supprimant dans le texte que la modification des droits d'accès ne s'applique pas au médecin référent et aux professionnels d'un service d'urgence d'un établissement hospitalier. En effet, le nouveau texte permet au titulaire d'interdire l'accès à son dossier intégral à des professionnels de santé qu'il désigne expressément ou de rendre certaines données inaccessibles à certains professionnels de santé, sans exception. Comme le précise le commentaire de l'amendement respectif, *« cette modification tient compte de la remarque du Conseil d'Etat qui soulève que la liste limitative de droits d'opposition est contraire à l'article 60quater, paragraphe 4 du Code de la sécurité sociale qui accorde un droit général au titulaire de pouvoir s'opposer à tout moment au partage de données le concernant. »*

Par ailleurs, la CNPD félicite les auteurs des amendements d'avoir ajouté à l'article 6 paragraphe (3) alinéa 4 du projet de règlement grand-ducal la possibilité pour le titulaire de demander l'effacement de ses données personnelles auprès du professionnel de santé ou de l'Agence eSanté. Or, similairement à ce que la CNPD avait constaté dans son avis du 5 avril 2018 dans le cadre de la possibilité pour le titulaire de rendre inaccessible certaines données spécifiques à un ou plusieurs professionnels de santé, la CNPD estime que la possibilité de demander l'effacement de données personnelles ne correspond pas à la réalité du système tel qu'il est conçu. Elle se demande notamment comment concrètement l'Agence eSanté ou les professionnels de santé entendent faire droit à des requêtes d'effacement de données personnelles spécifiques. En effet, le DSP ne contient que peu de données individuelles ou structurées, mais se compose en réalité et surtout de documents scannés, chaque document contenant une multitude d'informations ou de données de santé relatives à un patient.

La CNPD réitère donc son soucis de savoir comment il pourra être garanti qu'un titulaire puisse demander l'effacement de ses données personnelles (par exemple des données relatives à une interruption volontaire de grossesse) contenues dans plusieurs documents médicaux scannés. A moins de supprimer l'intégralité des documents, elle est d'avis qu'il ne sera pratiquement pas possible d'effacer certaines données spécifiques dans l'ensemble des documents contenant ces données spécifiques.

VI. Ad Amendement 8

Tout d'abord, la CNPD renvoie à son avis du 5 avril 2018, dans lequel elle avait déjà critiqué qu'une matrice des accès par défaut, comme celle prévue à l'annexe 1 du projet sous examen, doive par principe être considérée comme étant contraire au principe du « Privacy by Design » prévu par l'article 25 paragraphe (2) du RGPD.

Par ailleurs, l'article 7 nouveau paragraphe (1) alinéa 2 du projet de règlement grand-ducal prévoit des modalités spécifiques pour le « *classement d'un type de donnée au sein d'une catégorie de données* ». Etant donné que dans le DSP figurent surtout des documents scannés qui ne présentent aucune granularité, la CNPD rappelle que le texte du projet ne correspond pas à la réalité de la configuration des systèmes mis en place. Elle se demande

notamment comment l'Agence eSanté en tant que responsable du traitement va maîtriser la situation dans laquelle plusieurs catégories de données se retrouvent dans un même document scanné et qu'un professionnel de santé n'a droit d'accéder uniquement à une catégorie, mais non pas à une autre ?

De même, la CNPD a déjà eu l'occasion de souligner[5] que la liste des destinataires ne devrait pas à l'avenir être élargie à d'autres catégories de personnes (comme notamment des compagnies d'assurances privées, des employeurs, des praticiens de la médecine agissant en tant qu'expert pour le compte de tiers, etc.) et elle avait proposé aux auteurs d'ajouter une disposition dans ce sens dans le corps du texte du projet de règlement grand-ducal sous avis. Or, les auteurs des amendements n'ont pas tenu compte de cette recommandation.

En ce qui concerne le droit à l'information des personnes concernées, la CNPD note avec satisfaction que le paragraphe (3) nouveau de l'article 7 du projet de règlement grand-ducal impose dorénavant aux professionnels de santé l'obligation de fournir aux titulaires au moment de la collecte de leurs données, les informations visées à l'article 13, paragraphes 1 et 2 du RGPD. Néanmoins, la CNPD tient à insister que cette obligation d'informer les titulaires d'un DSP s'impose aussi à une collectivité de santé (par exemple un laboratoire, un centre d'aide et de soins, etc.). Il est primordial que le patient comprenne qu'une collectivité de santé, voire un professionnel de santé exerçant à titre individuel, entend accéder à son DSP et qu'il a la possibilité de refuser cet accès.

Finalement, pour répondre aux exigences légales du RGPD, un professionnel de santé, exerçant à titre individuel ou dans une collectivité de santé, devra être en mesure de démontrer que cette information au patient a bien eu lieu. La CNPD rappelle dans ce contexte sa recommandation déjà formulée en 2010 que le recours à une « carte de santé » de type « carte vitale française » ou « elektronische Gesundheitskarte » allemande faciliterait ce procédé, de même qu'une telle carte faciliterait l'utilisation d'autres procédés / fonctionnalités dans le cadre du système du DSP (tel que par exemple le recours à un identifiant de connexion peu pratique ou convivial).

VII. Ad amendement 10

Déjà dans son avis du 5 avril 2018, la CNPD a estimé que sur base des principes de minimisation des données et de la limitation de la conservation (article 5 paragraphe (1) lettres c) et e) du RGPD) et en considérant que le DSP a comme finalité principale le partage et l'échange de données utiles et pertinentes entre professionnels de santé pour une meilleure qualité de soins, que le DSP n'a pas comme vocation d'être exhaustif, qu'il ne se substitue pas aux dossiers tenus par les professionnels de santé ou les établissements hospitaliers et qu'il n'a certainement pas une finalité de stockage ou d'archivage de données, qu'une durée de conservation de cinq ans à compter du versement des données dans le DSP est suffisante et appropriée au regard des finalités réellement et légalement poursuivies.

Le Conseil d'Etat avait formulé des réserves similaires dans son avis du 23 octobre 2018 en estimant que la disposition concernant la durée de conservation générale de 10 ans *« manque de flexibilité et que le professionnel de santé qui introduit une donnée devrait pouvoir déterminer la durée de conservation de la donnée en fonction de son utilité et de sa pertinence,*

[5] Voir la délibération n° 345/2010 du 24 novembre 2010 relatif au projet de loi n°6196 portant réforme du système de soins de santé, ainsi que la délibération n° 242/2018 du 5 avril 2018 sur le projet de règlement grand-ducal sous examen.

et partant, fixer la date de son effacement en concertation avec le titulaire, date qui pourra, le cas échéant, être modifiée par la suite selon l'évolution de l'état de santé du titulaire. »

La CNPD note que même si la durée de conservation générale de 10 ans a été maintenue, par l'introduction du paragraphe (5) alinéa 2 de l'article 9 nouveau, le professionnel de santé peut, avec l'accord du titulaire, déroger à ce délai et déterminer une durée de conservation plus courte en fonction de l'utilité et de la pertinence de la donnée pour l'état de santé du titulaire. Par ailleurs, la CNPD félicite les auteurs des amendements d'avoir prévu à alinéa 3 dudit paragraphe que le professionnel de santé peut, avec l'accord du titulaire, déterminer que certaines données médicales jugées utiles et pertinentes à vie pour l'état de santé du titulaire, sont conservées jusqu'à la fermeture du dossier de soins partagé. Par ailleurs, il est précisé que *« l'accord du titulaire est daté et consigné dans son espace d'expression personnelle dans l'application dossier de soins partagé. »*

VIII. Ad amendement 11

L'amendement 11 vise à modifier l'article 10 du projet de règlement grand-ducal concernant la sécurité de la plateforme.

Dans son avis du 5 avril 2018, la CNPD avait critiqué qu'en ce qui concerne particulièrement les éditeurs d'un programme informatique connecté à la plateforme nationale, on pourrait interpréter l'ancien article 11 paragraphe (2) du projet de telle manière que ces derniers pourraient se connecter directement à la plateforme. Or, la CNPD avait souligné qu'il n'est pas acceptable que des acteurs IT aient eux-mêmes un accès direct au DSP, ceci n'étant absolument pas la pratique en la matière.

La CNPD prend note que par l'amendement 11, le terme précité de l'« éditeur d'un programme informatique » est remplacé par le terme « sous-traitant » dans le paragraphe 2, alinéa 1 et 3, et les auteurs expliquent dans le commentaire « *qu'il est admis que les prestataires aient besoin dans l'exécution des missions leur attribuées dans le cadre de l'application dossier de soins partagés, pour des raisons techniques et organisationnelles, de sous-traitants leur mettant en place des mesures de sécurité pour garantir la disponibilité, l'authenticité, l'intégrité, la confidentialité et la traçabilité des données échangées sur la plateforme.* »

La CNPD tient à réitérer dans ce contexte ses réserves concernant l'accès aux DSP par des acteurs autres que les professionnels de santé. Le projet actuel ne fournit à cet égard aucun encadrement législatif qui irait au-delà des principes généraux prévus au RGPD, notamment en matière de sous-traitance (article 28 du RGPD). Or, un accès à une grande partie des données de santé de la population quasi-entière justifierait et rendrait nécessaire une telle précision. A titre d'exemple, la CNPD se réfère aux mesures législatives qui ont été prises au niveau du secteur bancaire pour encadrer et protéger l'accès aux données financières. Selon l'avis de la CNPD, les données de santé, spécifiquement réglementées par l'article 9 du RGPD, sont d'une sensibilité supérieure aux données financières – et devraient de ce fait faire l'objet d'une protection tout au moins équivalente. Sans vouloir être exhaustif, la CNPD attire aussi l'attention sur le fait que dans d'autres Etats membres des mécanismes d'accréditation permettent d'assurer à ce que l'accès à de telles données soit soumis à un contrôle indépendant ou tout au moins sous le contrôle de l'Etat.

La CNPD rappelle que sans encadrement supplémentaire chaque prestataire de santé peut recourir à des sous-traitants sur base de sa propre évaluation de risque – tout en exposant potentiellement l'intégralité des données contenues au DSP. La situation actuelle, se

manifestant par une absence de pouvoir de l'Agence eSanté de contrôler qui a accès au système du DSP, rendrait donc quasiment impossible tout pouvoir de ladite Agence d'assurer un niveau élevé de sécurité du système.

Finalement, la Commission nationale constate qu'une grande partie de ses recommandations ou questions concernant l'actuel article 10 sur la sécurité de la plateforme n'ont pas été prises en compte par les auteurs des amendements.

Ainsi, la Commission nationale tient à rappeler certaines de ses observations formulées dans son avis précité concernant l'ancien article 11 intitulé : « Sécurité de la plateforme électronique nationale » :

« Selon l'article 11 paragraphe (1) du projet, l'Agence eSanté s'engage à mettre en œuvre un système de management de la sécurité de l'information certifié conforme à la Norme internationale ISO/IEC 27001. Néanmoins, la CNPD suggère de préciser dans le texte du projet de règlement grand-ducal le périmètre minimum sur lequel ladite certification ISO devra se porter. Le périmètre devra porter sur l'intégralité des systèmes, processus et éléments organisationnels impliqués directement ou indirectement sur la plateforme et reflétant bien, le cas échéant, la situation de la responsabilité conjointe.

L'article 11 paragraphe (1) lettre e) du projet envisage la « mise en place d'audits de sécurité annuels ». L'article 32 paragraphe (1) du RGPD contient dans ce contexte une liste non exhaustive de mesures techniques et organisationnelles que le responsable du traitement et le sous-traitant doivent mettre en œuvre afin de garantir un niveau de sécurité adapté au risque. Une de ces mesures est précisément la mise en place d'une « procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement » (article 32 paragraphe (1) lettre d) du RGPD). Si les auteurs du projet de règlement grand-ducal sous avis entendent viser cette disposition du RGPD, ils devraient en préciser les détails dans le corps du texte. Entre autres, la CNPD estime nécessaire de définir si ces audits seront effectués par des auditeurs indépendants ou par des auditeurs externes à l'Agence eSanté. De même, le projet reste muet sur le périmètre spécifique de ces audits, alors qu'une approche régulièrement adoptée en la matière se manifeste par un plan d'audit tri-annuel validé par le conseil d'administration pour qu'au bout de 3 ans, toutes les procédures ont été auditées.

Le paragraphe (2) dudit article oblige les prestataires et éditeurs d'un programme informatique connecté à la plateforme nationale à mettre en œuvre des mesures de sécurité appropriées au regard de son type, de sa taille, de ses processus ou de ses activités. Or, la CNPD est d'avis que la taille du prestataire ou éditeur n'est pas à considérer comme un critère pertinent dans ce contexte. En effet, l'article 32 paragraphe (1) du RGPD précise que les mesures techniques et organisationnelles à mettre en place doivent être adaptées à « l'état des connaissances, des coûts de mise en oeuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques [...]. » Le risque peut par exemple être particulièrement élevé si un prestataire a accès à un grand nombre de DSP.

[...]

Enfin, la Commission nationale se demande à quelles intervalles l'Agence eSanté entend mettre en œuvre les mesures de sensibilisation du personnel telles que prévues à l'article 11 paragraphe (2) lettre e) du projet. »

IX. Ad amendement 12

L'amendement 12 vise à modifier certains termes de l'ancien article 12 intitulé « Modalités techniques de versement des données au dossier de soins partagé et interopérabilité » du projet de règlement grand-ducal qui devient le nouvel article 11 du projet de règlement grand-ducal.

La Commission nationale constate dans ce contexte qu'aucune de ses remarques n'a été considérée par les auteurs des amendements.

Ainsi, la Commission nationale tient à réitérer ses observations formulées dans son avis précité concernant l'ancien article 12 intitulé « Modalités techniques de versement des données au dossier de soins partagé et interopérabilité » :

« Selon l'article 12 paragraphe (2) alinéa 4 lettre a) du projet, les tests mentionnés au paragraphe 2, alinéa 3 lettre a) dudit article seront effectués non pas par l'Agence eSanté, mais par un organisme ou une société experte en interopérabilité des systèmes de santé. La CNPD se pose surtout la question qui devra assumer les frais concernant les travaux de cet expert, et surtout qui désignera cet expert et sur base de quels critères les compétences de ce dernier seront vérifiées ?

Le paragraphe (2) de l'article 12 du projet continue en ce sens qu'une attestation de conformité sera délivrée par l'Agence eSanté sur base du résultat des tests réalisés par l'expert susmentionné. Or, sur quels critères l'Agence eSanté va-t-elle baser sa décision et comment va-t-elle se décider concrètement ? Est-ce que des représentants ne faisant pas partie de l'Agence eSanté seront impliqués pour garantir l'indépendance de la décision? La CNPD recommande ainsi aux auteurs d'indiquer dans le projet que l'Agence eSanté doit mettre en place un règlement d'ordre intérieur fixant les procédures de délivrance, de blocage et de retrait des attestations afin de garantir une équité de traitement des attestations pour tous les acteurs.

Enfin, dans l'article 12 paragraphe (2) alinéa 6 du projet il est indiqué que l'attestation des résultats des tests reste valable tant qu'aucune modification ne l'affecterait. Or cette approche ne correspond pas au bonnes pratiques en la matière, car même sans changement dans les systèmes, des nouvelles vulnérabilités dans des applications existantes pourraient tout à fait être découvertes et par la suite potentiellement exploitées. Ainsi la CNPD estime qu'une « procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement » telle que préconisée dans l'article 32 (1) (d) du RGPD devrait être mise en place – et ceci indépendamment si des modifications ont eues lieu. »

Ainsi décidé à Esch-sur-Alzette en date du 18 octobre 2019.

La Commission nationale pour la protection des données

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann	Marc Lemmer
Présidente	Commissaire	Commissaire	Commissaire